АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптографические протоколы и стандарты»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины:

- изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи изучения дисциплины:

- обучить студентов принципам работы основных протоколов;
- привить студентам навыки реализации криптографических протоколов с использованием ЭВМ;
- дать студентам представление об анализе стойкости протоколов к атакам.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к базовой части цикла Б1 образовательной программы и читается в 8-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра и геометрия», «Дискретная математика», «Криптографические методы защиты информации», «Информатика».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Методы алгебраической геометрии в криптографии», «Дополнительные главы криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины «Криптографические протоколы и стандарты» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-1 – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	Уметь: применять математические методы исследования моделей шифров
ОПК-2 – способностью корректно применять	Знать:

при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования
ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать: основные задачи и понятия криптографии
ПК-13 – способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать: требования к шифрам и основные характеристики шифров
ПК-15 – способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров
ПК-22 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Знать: основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
ПК-26 – способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами;
ПК-27 – способностью выполнять полный	Знать:

объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	типовые шифры с открытыми ключами Уметь: навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров
ПСК-4.1 – способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПСК-4.2 – способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПСК-4.3 – способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление;
- выполнение курсовой работы.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, проверка решения задач.

Итоговая аттестация проводится в форме: экзамен.